# Zeszyt ćwiczeń

## Cyberbezpieczeństwo w firmie: szkolenie dla pracowników i kadry zarządzającej (NIS2)

Kurs VITA: vita.edu.pl/courses/cyberbezpieczenstwo-w-firmie-dla-pracownikow-i-kadry
24 ćwiczenia, po jednym do każdej lekcji. Na końcu znajdziesz przykładowe odpowiedzi. Najpierw spróbuj odpowiedzieć samodzielnie, dopiero potem zajrzyj do wzorów. Postacie i sytuacje w ćwiczeniach są przykładowe. Zeszyt jest materiałem edukacyjnym, nie poradą prawną ani konsultacją specjalisty, i nie zastępuje prawnika, inspektora ochrony danych ani działu IT. Stan prawny: listopad 2026.

# Ćwiczenia

## Moduł 1. Zagrożenia w firmie: phishing, oszustwa na prezesa, wycieki

### Lekcja 1.1. Jakie zagrożenia dotyczą pracownika: phishing, vishing, oszustwo na prezesa, wyciek

Przypisz każdą z czterech sytuacji do rodzaju zagrożenia i napisz, co zrobisz jako pierwszy krok: 1) SMS z linkiem "dopłać 1,50 zł do paczki, inaczej zwrot do nadawcy". 2) Telefon od "konsultanta dostawcy internetu", który prosi o zainstalowanie programu do zdalnej pomocy. 3) Mail z adresu podobnego do adresu prezesa: "Zrób dziś przelew 18 400 zł, nie dzwoń, jestem na spotkaniu". 4) Wysyłasz ofertę z danymi klienta i dopiero po kliknięciu widzisz, że adres odbiorcy jest błędny.

### Lekcja 1.2. Jak wygląda atak krok po kroku: oś czasu od wiadomości do straty

Zapisz własną oś czasu z czterech punktów dla sytuacji: dostajesz mail z "umową do podpisu" od rzekomego kontrahenta. Przy każdym punkcie wpisz, co robisz, żeby zatrzymać łańcuch.

### Lekcja 1.3. Przypadek: pilny przelew "od prezesa" w piątek po 16:00

Zapisz, jak w Twoim zespole wyglądałaby zasada potwierdzania przelewu na nowy rachunek: od jakiej kwoty, przez kogo, jakim kanałem i co zapisujesz po potwierdzeniu. Napisz jedną zasadę w trzech zdaniach.

## Moduł 2. Hasła, uwierzytelnianie dwuskładnikowe i konta służbowe

### Lekcja 2.1. Hasła i weryfikacja dwuetapowa: zasady CERT Polska

Ułóż hasło z co najmniej czterech słów, które mają dla Ciebie sens, ale nie opisują Twoich danych osobowych (bez imion bliskich, dat urodzin, nazwy firmy). Potem wypisz pięć kont służbowych i oznacz, na których włączysz weryfikację dwuetapową w tym tygodniu.

### Lekcja 2.2. Zasady kont służbowych: wzór krótkiej polityki haseł i dostępów dla zespołu

Napisz własną wersję punktu 6 polityki (odejście lub zmiana stanowiska) dla zespołu pięciu osób, który korzysta z poczty, programu do fakturowania i dysku sieciowego. Podaj, kto zgłasza, komu, w jakim terminie i co zostaje odebrane.

### Lekcja 2.3. Przypadek: współdzielone konto w zespole i odejście pracownika

Wskaż jedno konto współdzielone w Twoim zespole (lub wymyśl realistyczne) i napisz plan jego zastąpienia: kto zna hasło, jakie konta imienne trzeba założyć, kiedy zmienisz hasło i kto sprawdzi to za pół roku.

## Moduł 3. Poczta, linki i załączniki: jak sprawdzić wiadomość

### Lekcja 3.1. Sprawdzanie wiadomości: nadawca, link, załącznik, ton pilności

Przykład fikcyjny: w skrzynce pani Haliny z firmy Drewmax w Poznaniu pojawia się wiadomość "Wezwanie do zapłaty, ostatnia szansa dziś". Nazwa nadawcy to "Dział windykacji Mazovia-Trans", w treści jest link do płatności i załącznik wezwanie.pdf.exe. Wypisz, co sprawdzisz w każdym z czterech miejsc, i napisz, co zrobisz dalej.

### Lekcja 3.2. Wzór zgłoszenia podejrzanej wiadomości do działu IT i co powiedzieć rozmówcy przez telefon

Przykład fikcyjny: w poniedziałek o 9:05 pani Weronika, księgowa w firmie Kolbud w Gdyni, dostaje maila z adresu zaplaty@kolbud-faktury.example z załącznikiem "korekta.zip". Hasło do archiwum jest w treści. Otworzyła archiwum i

zobaczyła jeden plik .scr, którego nie uruchomiła. Napisz jej zgłoszenie do działu IT według wzoru.

### Lekcja 3.3. Przypadek: faktura w archiwum ZIP z hasłem w treści maila

Przykład fikcyjny: pan Krzysztof z sekretariatu firmy Mazur-Okna w Lublinie dostaje mail "Zamówienie do potwierdzenia" z załącznikiem zamowienie.docx. Po otwarciu dokument pokazuje rozmazany tekst i napis "Włącz zawartość, aby wyświetlić". Napisz, co pan Krzysztof powinien zrobić i w jakiej kolejności, jeśli jeszcze nie kliknął przycisku.

## Moduł 4. Praca zdalna, urządzenia prywatne i publiczne sieci

### Lekcja 4.1. Praca poza biurem: sieć domowa, publiczne Wi-Fi, VPN, blokada ekranu

Przygotuj własną listę pięciu pytań przed pracą poza biurem, dopasowaną do Twojego stanowiska: wybierz co najmniej jedną zasadę dotyczącą sieci, jedną dotyczącą ekranu i jedną dotyczącą tego, co zabierasz ze sobą.

### Lekcja 4.2. Urządzenia prywatne w pracy: zasady BYOD i wzór oświadczenia lub reguł dla zespołu

Napisz własne trzy reguły dla prywatnego urządzenia w swoim zespole oraz jedno zdanie oświadczenia, które pracownik podpisze. Trzy reguły mają odpowiadać na trzy różne ryzyka: dostęp osoby trzeciej, zgubienie urządzenia i przechowywanie plików firmy poza systemem firmowym.

### Lekcja 4.3. Przypadek: zgubiony laptop w pociągu z danymi klientów

Przykład fikcyjny: pani Agata z firmy Lokomo w Katowicach zgubiła służbowy telefon z pocztą, w której są dane osobowe klientów. Telefon miał blokadę PIN, ale nie wiadomo, czy był szyfrowany. Napisz pierwsze cztery działania w kolejności i wskaż, kto ocenia sprawę pod kątem RODO.

## Moduł 5. Dane i RODO: incydent, zgłoszenie, kto co robi

### Lekcja 5.1. Naruszenie ochrony danych w RODO: czym jest, art. 33 i 34, rola pracownika

Wypisz trzy zdarzenia ze swojej pracy z ostatniego roku (lub możliwe do wyobrażenia), w których mogło dojść do naruszenia ochrony danych osobowych, i przy każdym wskaż, które z pięciu zdarzeń z art. 4 pkt 12 zachodzi (zniszczenie, utrata, zmodyfikowanie, nieuprawnione ujawnienie, nieuprawniony dostęp) oraz komu w firmie zgłosisz je jako pierwszemu.

**Przykładowa odpowiedź (przykład fikcyjny):** 1) Mail z listą zamówień wysłany do niewłaściwego kontrahenta: nieuprawnione ujawnienie, zgłaszam przełożonej i IOD. 2) Służbowy telefon z pocztą zgubiony w tramwaju w Łodzi: utrata, nieuprawniony dostęp możliwy, zgłaszam do działu IT i przełożonej. 3) Plik z grafikiem urlopów nadpisany przez nieuprawnioną osobę: zmodyfikowanie, zgłaszam przełożonemu.

### Lekcja 5.2. Rejestr naruszeń i wzór wewnętrznego zgłoszenia pracownika

Napisz własne zgłoszenie według ośmiu pól dla zdarzenia: wracasz z konferencji w Poznaniu i orientujesz się, że służbowy tablet z listą 120 kontaktów do klientów (imię, firma, telefon, mail) został w taksówce. Wypełnij pola 3 do 8, a daty i godziny wpisz przykładowe.

### Lekcja 5.3. Przypadek: mail z danymi klientów wysłany do złego odbiorcy

Zastosuj przypadek do siebie: wypisz po jednym zdaniu, co zrobisz w pierwszych pięciu minutach po zauważeniu, że wysłałeś plik z danymi klientów pod zły adres, oraz trzy pytania, które zadasz odbiorcy lub IOD.

## Moduł 6. NIS2 i ustawa o krajowym systemie cyberbezpieczeństwa: obowiązki firmy i kadry zarządzającej

### Lekcja 6.1. NIS2 i KSC w pigułce: kogo dotyczą, podmiot kluczowy i ważny, terminy przejściowe

Wypełnij kartę wstępnej oceny dla firmy, w której pracujesz: PKD głównej działalności, sektor w załączniku nr 1 lub 2 (tak, nie, nie wiem), wielkość (zatrudnienie, przychód), czy firma ma wpis w wykazie, kto jest osobą do kontaktu z prawnikiem. Nie wpisuj wniosku końcowego, tylko listę pytań do sprawdzenia.

**Przykładowa odpowiedź (przykład fikcyjny):** Biuro projektowe Trzy Pola z Lublina, 12 osób. PKD: działalność architektoniczna. Sektor w załączniku: nie widzę, do sprawdzenia z prawnikiem. Wielkość: mała firma, dane od księgowej. Wpis w wykazie: brak informacji. Pytania: czy któryś z klientów, na przykład z sektora energii, wymaga w umowie spełnienia zasad bezpieczeństwa; czy firma korzysta z usług, które mają własne wymagania. Decyzja o statusie należy do firmy po konsultacji z prawnikiem.

### Lekcja 6.2. Obowiązki kierownika: art. 8c, 8d, 8e i dokumentowanie szkoleń (wzór listy obowiązków)

Przygotuj listę obowiązków kierownika (min. cztery wiersze) dla fikcyjnej firmy Zakład Opakowań Nadodrze sp. z o.o. we Wrocławiu, zarząd dwuosobowy: Elżbieta Witkowska (prezes) i Tomasz Gajda (wiceprezes). Do każdego wiersza dopisz podstawę, osobę i dowód.

**Przykładowa odpowiedź (przykład fikcyjny):** 1) Decyzje o SZBI: art. 8d pkt 1; prezes E. Witkowska; protokół zarządu z kwartalnego przeglądu. 2) Budżet: art. 8d pkt 2; wiceprezes T. Gajda; pozycja w rocznym planie finansowym. 3) Zadania i nadzór: art. 8d pkt 3; wiceprezes T. Gajda; zakresy obowiązków kierownika IT, spotkanie raz na miesiąc. 4) Świadomość personelu: art. 8d pkt 4; HR; lista uczestników szkolenia z datą i tematem. 5) Szkolenie zarządu: art. 8e; oboje członkowie; wpis do rejestru i certyfikat. Gdyby zarząd nie wskazał osoby odpowiedzialnej, według art. 8c ust. 2 odpowiadałyby obie osoby.

### Lekcja 6.3. Przypadek: zarząd średniej firmy pyta, czy jest objęty ustawą i co zrobić w tym kwartale

Przygotuj plan na kwartał dla własnego zespołu lub zarządu: cztery zadania z terminem, osobą i dowodem wykonania. Pierwsze zadanie ma dotyczyć ustalenia statusu firmy, a ostatnie harmonogramu dalszych prac.

## Moduł 7. Reagowanie na incydent: pierwsze godziny i komunikacja

### Lekcja 7.1. Pierwsze godziny po incydencie: co robi pracownik, co robi IT, co robi zarząd; terminy 24 h, 72 h

Przykład fikcyjny: w firmie Bramka Sp. z o.o. w Poznaniu księgowa Halina o 9:20 wpisała hasło na stronie, która okazała się fałszywa. Wypisz, co robi ona, co robi IT (Marcin) i co robi prezes (Wojciech) w pierwszej godzinie, oraz które terminy trzeba sprawdzić. Załóż, że firma jest objęta KSC i że w systemie księgowym są dane osobowe klientów.

### Lekcja 7.2. Plan reakcji na incydent: karta pierwszych działań i komunikat do zespołu (wzór)

Napisz komunikat do zespołu w czterech zdaniach dla sytuacji: o 10:15 przestała działać poczta firmowa w 30-osobowej firmie z Wrocławia, IT potwierdza, że kilka kont zostało przejętych po wpisaniu haseł na fałszywej stronie. Dodaj godzinę następnej informacji i jedną osobę do pytań z zewnątrz.

### Lekcja 7.3. Przypadek: ransomware w piątek wieczorem, kto dzwoni do kogo

Zdarzenie wykryto w piątek o 21:15. Wypisz kolejno: komu zgłasza pracownik, kto powiadamia zarząd, do kiedy upływa termin wczesnego ostrzeżenia i zgłoszenia incydentu poważnego (KSC) oraz co jeszcze trzeba ocenić w sobotę rano w związku z RODO. Dodaj jeden element, który musi być w planie na weekend.

## Moduł 8. Projekt końcowy: plan szkolenia i zasady bezpieczeństwa w

## moim zespole

### Lekcja 8.1. Projekt: ocena ryzyk w moim zespole (3 najważniejsze zagrożenia i kto za nie odpowiada)

Przygotuj tabelę ryzyk dla własnego zespołu (lub fikcyjnego zespołu pięciu osób w dziale sprzedaży). Wybierz trzy zagrożenia z modułów 1-7, dla każdego wpisz prawdopodobieństwo, skutek, środek, który działa dziś, oraz osobę odpowiedzialną z imienia i roli. Dopisz jedno zagrożenie, które świadomie odkładasz, wraz z powodem.

### Lekcja 8.2. Projekt: plan szkolenia i zasad bezpieczeństwa (dokument do użycia w firmie)

Napisz dokument dla zespołu pięciu osób w księgowości, korzystając z pól z tej lekcji: trzy zasady dopasowane do trzech ryzyk (oszustwo na fakturze, błędnie wysłany mail, praca zdalna), plan z trzema terminami i dowodami udziału, role z imionami oraz data przeglądu. Zasady muszą dać się sprawdzić w pracy, a każdy termin ma mieć datę.

### Lekcja 8.3. Projekt: jak wdrożyć plan, mierzyć efekt i co powtarzać co roku

Ułóż harmonogram wdrożenia planu swojego zespołu na 90 dni (trzy odcinki z datami), wybierz trzy mierniki z miejscem, z którego weźmiesz dane, i zapisz datę rocznego przeglądu wraz z pięcioma pytaniami do niego. Dołącz jedno zdanie, które powiesz zespołowi na spotkaniu wprowadzającym.

# Przykładowe odpowiedzi

## Moduł 1. Zagrożenia w firmie: phishing, oszustwa na prezesa, wycieki

### Lekcja 1.1. Jakie zagrożenia dotyczą pracownika: phishing, vishing, oszustwo na prezesa, wyciek

Rozwiązanie: 1) Phishing: nie klikasz, usuwasz wiadomość, ewentualnie zgłaszasz ją w dziale IT. 2) Vishing: rozłączasz się, nie instalujesz niczego, oddzwaniasz na numer ze strony dostawcy i informujesz dział IT. 3) Oszustwo na prezesa: nie robisz przelewu, dzwonisz do prezesa na jego znany numer i zgłaszasz wiadomość. 4) Wyciek: od razu zawiadamiasz osobę wskazaną w procedurze (zwykle przełożonego lub IOD), podajesz, co wysłano, do kogo i kiedy, bez usuwania śladów.

Do kursu dołączono zeszyt ćwiczeń z 24 zadaniami i rozwiązaniami. Pobierzesz go tutaj: [Zeszyt ćwiczeń: cyberbezpieczeństwo w firmie](/downloads/zeszyt-cwiczen-cyberbezpieczenstwo-w-firmie.pdf). Wydrukuj go i wypełniaj na bieżąco.

### Lekcja 1.2. Jak wygląda atak krok po kroku: oś czasu od wiadomości do straty

Przykładowa odpowiedź: 1) Wiadomość: sprawdzam pełny adres nadawcy i porównuję z poprzednią korespondencją z kontrahentem. 2) Link lub załącznik: nie klikam, jeśli adres jest inny; dzwonię do kontrahenta na znany numer i pytam, czy wysłał umowę. 3) Podejrzenie po kliknięciu: od razu piszę do działu IT, podaję godzinę i to, co wpisałem. 4) Prośba o zmianę rachunku lub przelew: potwierdzam telefonicznie, zanim ktokolwiek wykona płatność.

### Lekcja 1.3. Przypadek: pilny przelew "od prezesa" w piątek po 16:00

Przykładowa odpowiedź: "Przelew na rachunek, którego wcześniej nie było w systemie, wymaga potwierdzenia telefonicznego przez drugą osobę upoważnioną, bez względu na kwotę. Potwierdzenie następuje na numer zapisany w firmowej książce adresowej, nigdy na numer z wiadomości z prośbą o płatność. Osoba wykonująca przelew zapisuje datę, godzinę i imię osoby, która potwierdziła, w rejestrze płatności."

## Moduł 2. Hasła, uwierzytelnianie dwuskładnikowe i konta służbowe

### Lekcja 2.1. Hasła i weryfikacja dwuetapowa: zasady CERT Polska

Przykładowa odpowiedź: Hasło: "BurzaNadRzekaZnalazlaMostek" (27 znaków, pięć słów, bez danych osobowych; to wzór układu, własne hasło ułóż inaczej i nie używaj przykładu). Konta: 1) poczta firmowa, weryfikacja włączona od razu. 2) Bankowość firmy, od razu. 3) System księgowy, w tym tygodniu. 4) Panel z danymi klientów, w tym tygodniu. 5) Konto w mediach społecznościowych firmy, w następnym tygodniu.

### Lekcja 2.2. Zasady kont służbowych: wzór krótkiej polityki haseł i dostępów dla zespołu

Przykładowa odpowiedź: "Kierownik zespołu zgłasza w dziale IT odejście lub zmianę stanowiska pracownika najpóźniej w dniu poprzedzającym ostatni dzień pracy. W dniu ostatniej pracy dział IT odbiera dostęp do poczty, programu do fakturowania i dysku sieciowego, a kierownik zapewnia przekazanie bieżących spraw innej osobie. Po odebraniu dostępów dział IT potwierdza to mailem kierownikowi."

### Lekcja 2.3. Przypadek: współdzielone konto w zespole i odejście pracownika

Przykładowa odpowiedź: Konto: wspólna skrzynka "zamowienia@" w firmie handlowej, hasło zna pięć osób. Plan: dział IT zamienia ją w skrzynkę udostępnioną, do której każda z pięciu osób loguje się własnym kontem; stare hasło zostaje zmienione i zapisane w menedżerze haseł tylko u kierownika; zmianę wykonujemy w tym tygodniu; kierownik za pół roku porównuje listę osób z dostępem z listą osób w zespole i usuwa różnice.

## Moduł 3. Poczta, linki i załączniki: jak sprawdzić wiadomość

### Lekcja 3.1. Sprawdzanie wiadomości: nadawca, link, załącznik, ton pilności

Rozwiązanie: Nadawca: rozwijam pełny adres e-mail i porównuję z adresem kontrahenta, jeśli taki istnieje w naszej bazie. Link: najeżdżam kursorem, nie klikam, nie płacę. Załącznik: końcówka .pdf.exe oznacza plik wykonywalny, nie dokument, więc nie otwieram. Ton: "ostatnia szansa dziś" to presja czasu. Dalej: zgłaszam wiadomość do działu IT, a jeśli firma Mazovia-Trans jest naszym realnym kontrahentem, dzwonię do niej na numer z jej strony internetowej.

### Lekcja 3.2. Wzór zgłoszenia podejrzanej wiadomości do działu IT i co powiedzieć rozmówcy przez

**telefon**

Przykładowa odpowiedź: Zgłoszenie podejrzanej wiadomości. Data i godzina otrzymania: poniedziałek, 9:05. Mój adres: służbowy, księgowość. Adres nadawcy: zaplaty@kolbud-faktury.example. Temat: korekta faktury. Co zawierała: archiwum korekta.zip z hasłem podanym w treści, w środku plik z końcówką .scr. Co zrobiłem: otworzyłem archiwum o 9:12, pliku nie uruchomiłem, niczego nie wpisywałem. Czy ktoś jeszcze mógł dostać: nie wiem, adres nie jest mi znany z poprzednich faktur. Weronika, telefon wewnętrzny.

### Lekcja 3.3. Przypadek: faktura w archiwum ZIP z hasłem w treści maila

Rozwiązanie: 1) Nie klika "Włącz zawartość", bo ten przycisk może uruchomić makra, czyli polecenia zapisane w pliku. 2) Zamyka dokument. 3) Sprawdza pełny adres nadawcy w wiadomości i porównuje z adresem klienta. 4) Dzwoni do klienta na numer z umowy, żeby sprawdzić, czy wysłał zamówienie. 5) Zgłasza wiadomość do IT według wzoru: godzina, adres nadawcy, nazwa pliku, "dokument otwarto, zawartości nie włączono". 6) Czeka na decyzję IT, co dalej robić z plikiem.

## Moduł 4. Praca zdalna, urządzenia prywatne i publiczne sieci

### Lekcja 4.1. Praca poza biurem: sieć domowa, publiczne Wi-Fi, VPN, blokada ekranu

Przykładowa odpowiedź: 1) Czy łączę się przez sieć domową lub VPN, zamiast przez otwarte Wi-Fi? 2) Czy ekran blokuje się sam po kilku minutach? 3) Czy wziąłem tylko pliki potrzebne na ten dzień? 4) Czy włączone jest logowanie dwuetapowe do poczty? 5) Czy mam numer do działu IT na wypadek zgubienia sprzętu?

### Lekcja 4.2. Urządzenia prywatne w pracy: zasady BYOD i wzór oświadczenia lub reguł dla zespołu

Przykładowa odpowiedź: 1) Telefon ma blokadę ekranu, której nie znają domownicy. 2) Zgubienie lub kradzież urządzenia zgłaszam do działu IT w dniu zdarzenia. 3) Pliki firmy otwieram w aplikacji służbowej i nie zapisuję ich w prywatnych chmurach ani na komunikatorach. Oświadczenie: "Zapoznałem się z regułami korzystania z prywatnego urządzenia do pracy i zobowiązuję się ich przestrzegać."

### Lekcja 4.3. Przypadek: zgubiony laptop w pociągu z danymi klientów

Rozwiązanie: 1) Pani Agata zgłasza zgubienie działowi IT tego samego dnia, podając godzinę, miejsce i opis zawartości telefonu. 2) IT blokuje urządzenie i konta oraz zmienia hasła do poczty. 3) Pani Agata szuka telefonu u przewoźnika lub w biurze rzeczy znalezionych. 4) Zarząd lub osoba odpowiedzialna za ochronę danych ocenia, czy to naruszenie ochrony danych, i dokumentuje decyzję. Jeśli naruszenie zostanie stwierdzone i ryzyko nie jest mało prawdopodobne, firma zgłasza je organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości w 72 godziny (art. 33 RODO).

## Moduł 5. Dane i RODO: incydent, zgłoszenie, kto co robi

### Lekcja 5.1. Naruszenie ochrony danych w RODO: czym jest, art. 33 i 34, rola pracownika

### Lekcja 5.2. Rejestr naruszeń i wzór wewnętrznego zgłoszenia pracownika

Rozwiązanie: 3) W sobotę 14.11 około 17:00 zostawiłem w taksówce tablet służbowy; zauważyłem o 17:40 po powrocie do hotelu. 4) Lista około 120 kontaktów: imię, nazwisko, firma, telefon, mail. Dane płatnicze i PESEL: nie ma, według mojej wiedzy. 5) Tablet służbowy, nr inwentarzowy z naklejki, zablokowany kodem, szyfrowanie: nie wiem. 6) Zadzwoniłem do firmy taksówkowej, poprosiłem o poszukiwanie, zgłosiłem sprawę do działu IT. 7) Dział IT i przełożony. 8) Nie wiem, czy ktoś odblokował tablet.

### Lekcja 5.3. Przypadek: mail z danymi klientów wysłany do złego odbiorcy

Przykładowa odpowiedź: Zatrzymuję się i nie usuwam wiadomości z folderu wysłanych. Dzwonię do przełożonego i piszę zgłoszenie według wzoru (godzina, dane, odbiorca, co zrobiłem). Proszę odbiorcę o usunięcie wiadomości i pisemne potwierdzenie. Pytania: czy plik został otwarty, czy ktoś go przekazał dalej, czy dane znajdują się na kopii zapasowej poczty odbiorcy.

## Moduł 6. NIS2 i ustawa o krajowym systemie cyberbezpieczeństwa: obowiązki firmy i kadry zarządzającej

### Lekcja 6.1. NIS2 i KSC w pigułce: kogo dotyczą, podmiot kluczowy i ważny, terminy przejściowe

### Lekcja 6.2. Obowiązki kierownika: art. 8c, 8d, 8e i dokumentowanie szkoleń (wzór listy obowiązków)

### Lekcja 6.3. Przypadek: zarząd średniej firmy pyta, czy jest objęty ustawą i co zrobić w tym kwartale

Przykładowa odpowiedź: 1) Zebrać dane o firmie (PKD, zatrudnienie, sprawozdanie finansowe) i zlecić opinię prawnika o statusie, do 27.11, osoba: wiceprezes, dowód: opinia na piśmie. 2) Wskazać osobę odpowiedzialną w zarządzie i przydzielić zadania, do 4.12, osoba: prezes, dowód: uchwała lub protokół. 3) Ustalić termin szkolenia zarządu i założyć rejestr szkoleń, do 15.12, osoba: HR, dowód: wpis w rejestrze. 4) Przygotować harmonogram prac do 3.04.2027 z kontrolą komunikatu ministra, do 31.12, osoba: dyrektor IT, dowód: plan zatwierdzony przez zarząd.

## Moduł 7. Reagowanie na incydent: pierwsze godziny i komunikacja

### Lekcja 7.1. Pierwsze godziny po incydencie: co robi pracownik, co robi IT, co robi zarząd; terminy 24 h, 72 h

Przykładowa odpowiedź: Halina: przerywa pracę na tym koncie, zgłasza Marcinowi telefonem i mailem, podaje godzinę 9:20 i nazwę strony, nie zmienia nic na własną rękę. Marcin: blokuje konto i zmienia hasło po ustaleniu zakresu, sprawdza logowania z ostatnich godzin, ocenia, czy zdarzenie spełnia progi incydentu poważnego i czy dotknęło dane osobowe, notuje czasy. Wojciech: dostaje informację w ciągu godziny, ustala, kto jest osobą odpowiedzialną za zgłoszenia, i pilnuje zegara. Terminy: jeśli to incydent poważny, 24 h wczesne ostrzeżenie i 72 h zgłoszenie od wykrycia (KSC); jeśli doszło do naruszenia ochrony danych, osobno 72 h do organu nadzorczego (RODO art. 33). Początek biegu ustala się od wykrycia lub stwierdzenia, więc godzinę 9:20 trzeba zapisać.

### Lekcja 7.2. Plan reakcji na incydent: karta pierwszych działań i komunikat do zespołu (wzór)

Przykładowa odpowiedź: "O 10:15 wykryliśmy, że kilka kont pocztowych w firmie zostało przejętych przez osoby z zewnątrz. Na ten moment dotyczy to poczty, system księgowy i magazynowy działają. IT blokuje przejęte konta i sprawdza, jakie wiadomości z nich wychodziły; kolejna informacja będzie o 12:00. Do tego czasu zmień hasło do poczty zgodnie z instrukcją IT, nie otwieraj wiadomości z prośbą o logowanie i zgłaszaj podejrzane maile na adres it@(adres firmy). Pytania od klientów kieruj do Anny Sobczak, nie odpowiadaj samodzielnie."

### Lekcja 7.3. Przypadek: ransomware w piątek wieczorem, kto dzwoni do kogo

Rozwiązanie: Pracownik odłącza urządzenie od sieci bez wyłączania i dzwoni na numer dyżurny IT. IT po wstępnej ocenie dzwoni do prezesa lub osoby z zarządu wskazanej w planie. Termin wczesnego ostrzeżenia mija w sobotę o 21:15 (24 h od wykrycia), termin zgłoszenia incydentu poważnego w poniedziałek o 21:15 (72 h). W sobotę rano trzeba ocenić, czy doszło do naruszenia ochrony danych osobowych; jeśli tak, liczy się osobno 72 h od stwierdzenia naruszenia (art. 33 RODO) i zapis w dokumentacji naruszeń. Element planu na weekend: zastępca osoby odpowiedzialnej za zgłoszenia wraz z dostępem do systemu zgłoszeniowego i telefonami do zarządu, zapisanymi poza pocztą firmową.

## Moduł 8. Projekt końcowy: plan szkolenia i zasady bezpieczeństwa w moim zespole

### Lekcja 8.1. Projekt: ocena ryzyk w moim zespole (3 najważniejsze zagrożenia i kto za nie odpowiada)

Przykładowa odpowiedź: 1) Oszustwo na prezesa (prośba o pilny przelew): prawdopodobieństwo wysokie, skutek wysoki, dziś brak zasady, odpowiada Krzysztof Malinowski, kierownik sprzedaży. 2) Wspólne konto do systemu ofert: średnie, średni skutek, dziś jedno hasło dla czterech osób, odpowiada Ewa Lis, specjalistka ds. ofert. 3) Zgubiony służbowy laptop z bazą klientów: średnie, wysoki, dziś brak szyfrowania dysku, odpowiada Krzysztof Malinowski w uzgodnieniu z IT. Odkładam: ransomware w serwerowni (niskie prawdopodobieństwo przy sprawnych kopiach zapasowych, temat do zgłoszenia zarządowi i IT).

### Lekcja 8.2. Projekt: plan szkolenia i zasad bezpieczeństwa (dokument do użycia w firmie)

Rozwiązanie: Zasady: 1) Zmianę numeru rachunku na fakturze potwierdzamy telefonem na numer z naszej bazy, nie z faktury. 2) Przed wysłaniem pliku z danymi klientów sprawdzamy odbiorcę w oknie adresu, a plik zabezpieczamy hasłem podanym innym kanałem. 3) Praca zdalna tylko z urządzenia służbowego, z blokadą ekranu po 5 minutach. Plan: 20 stycznia, cały zespół, 45 minut, fałszywe faktury, dowód: lista z podpisami; 17 marca, cały zespół, 30 minut,

bezpieczna wysyłka danych, dowód: notatka z ćwiczenia; 12 maja, kierowniczka Marta Zielińska, obowiązki kierownika, dowód: potwierdzenie ukończenia. Role: kierowniczka zatwierdza, Janusz Kowal pilnuje zasad, kontakt IT to numer dyżurny z karty reagowania. Przegląd: 20 stycznia przyszłego roku.

### Lekcja 8.3. Projekt: jak wdrożyć plan, mierzyć efekt i co powtarzać co roku

Rozwiązanie: Harmonogram: 5-16 lutego spotkanie wprowadzające i potwierdzenia zapoznania; 19 lutego-29 marca szkolenie 3 marca (45 minut) i ćwiczenie zgłaszania 24 marca; 1-30 kwietnia sprawdzenie zasad i poprawki. Mierniki: 1) liczba osób z potwierdzonym udziałem (lista obecności), 2) liczba zgłoszonych podejrzanych wiadomości w kwartale (skrzynka kontaktu IT), 3) czas od zauważenia do zgłoszenia w ćwiczeniu (karta reagowania). Przegląd: 15 lutego następnego roku, pytania: czy trzy ryzyka są nadal najważniejsze, czy zmienił się zespół, czy mamy nowe narzędzia, czy zasady działały, czy zmieniły się przepisy dotyczące firmy. Zdanie do zespołu: "Przez trzy miesiące sprawdzamy trzy zasady i liczymy zgłoszenia; zgłoszenie w godzinę to normalna praca, nie przyznanie się do błędu."

Cały zestaw zadań z rozwiązaniami masz w zeszycie ćwiczeń: [Zeszyt ćwiczeń: cyberbezpieczeństwo w firmie] (/downloads/zeszyt-cwiczen-cyberbezpieczenstwo-w-firmie.pdf). Wróć do niego przy rocznym przeglądzie.